

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>			1. CONTRACT ID CODE		PAGE <b>1</b> OF <b>2</b>				
2. AMENDMENT/MODIFICATION NO. <b>PS72</b>		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO. <b>21435188</b>		5. PROJECT NO. (If applicable)			
6. ISSUED BY <b>GSA/FEDSIM Acquisition (QF0B1E) 1800 F Street, NW, 3100 Washington, DC 20405 Contract Specialist Name: Leverne T Frierson Contract Specialist Phone: 999-999-9999</b>		CODE <b>47QFCA</b>		7. ADMINISTERED BY (If other than item 6)			CODE		
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and ZIP Code) <b>LEIDOS, INC. 9737 WASHINGTONIAN BLVD GAITHERSBURG, MD, 20878-7337 Phone: 571-526-6000 Fax: 571-526-6000</b>				(X)			9A. AMENDMENT OF SOLICITATION NO.		
				X			9B. DATED (SEE ITEM 11)		
							10A. MODIFICATION OF CONTRACT/ORDER NO. <b>GS00Q09BGD0039 / GSQ0017AJ0079</b>		
							10B. DATED (SEE ITEM 13) <b>08/31/2017</b>		
CODE		FACILITY CODE							
<b>11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS</b>									
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended, <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning ____ copies of the amendment; (b) By acknowledge receipt of this amendment on each of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.									
12. ACCOUNTING AND APPROPRIATION DATA (If required) <b>285F.Q00FB000.AA10.25.AF151.H08 Total Amount of MOD: (\$10,034.00)</b>									
<b>13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.</b>									
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.									
B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).									
X C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: <b>FAR 43.103(a)(3) Bilateral Modification and FAR 52.232-22 Limitation of Funds</b>									
D. OTHER (Specify type of modification and authority)									
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return ____ copies to the issuing office.									
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) <b>The purpose of this modification is stated in the attached SF 30 Continuation Page. See award documents for details.</b>									
Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.									
15A. NAME AND TITLE OF SIGNER (Type or print) <b>(b)(6)</b>				16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) <b>Nydia Roman-Albertorio</b>					
15B. CONTRACTOR/OFFEROR <b>(b)(6)</b> (Signature of person authorized to sign)		15C. DATE SIGNED <b>04/26/2021</b>		16B. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) <b>(b)(6)</b>		16C. DATE SIGNED <b>28 APR 2021</b>			

Line Item Summary							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	Rev. Ext. Price (F)	Prev. Ext. Price (G)	Amount Of Change (H)
0001a	CLIN 0001a FFP Labor (4 months Transition-in)	(b)(4)					
0001b	CLIN 0001b FFP Labor (8 months post-Transition-in)						
0002	CLIN 0002 Transition-in CPAF Labor						
0003	CLIN 0003 CPAF Labor (post-transition)						
0004	CLIN 0004 Travel						
0005	CLIN 0005 Tools						
0006	CLIN 0006 ODCs						
0007	CLIN 0007 Contract Access Fee						
0009	CLIN 0009 Non-Severable CPAF Labor						
0010	CLIN 0010 Non-Severable Travel						
0011	CLIN 0011 Non-Severable Tools						
0012	CLIN 0012 Non-Severable ODCs						
1001	CLIN 1001 OY1 FFP Labor						
1003	CLIN 1003 OY1 CPAF Labor						
1004	CLIN 1004 OY1 Travel						
1005	CLIN 1005 OY1 Tools						
1006	CLIN 1006 OY1 ODCs						
1007	CLIN 1007 OY1 Contract Access Fee						
2001	CLIN 2001 OY2 FFP Labor						
2003	CLIN 2003 OY2 CPAF Labor						
2004	CLIN 2004 OY2 Travel						
2005	CLIN 2005 OY2 Tools						
2006	CLIN 2006 OY2 ODCs						
2007	CLIN 2007 OY2 Contract Access Fee						
3001	CLIN 3001 OY3 FFP Labor						
3003	CLIN 3003 OY3 CPAF Labor						
3004	CLIN 3004 OY3 Travel						
3005	CLIN 3005 OY3 Tools						
3006	CLIN 3006 OY3 ODCs						
3007	CLIN 3007 OY3 Contract Access Fee						
TOTALS:					(b)(4)		(\$10,034.00)

**SF 30, Block 14 Continuation**  
**Contract No.: GS00Q09BGD0039**  
**Task Order: GSQ0017AJ0079**  
**Modification P00072**

The purpose of this modification is to: 1) De-obligate funding for Option Period 2 Severable CLINs; and 2) Incorporate Final Award Fee Report Package for Period 7 (8/31/2020 – 2/28/2021).

1. Attachment C, Incremental Funding Chart, is updated to de-obligate funding for Option Period 2 Severable CLINs 2003, and 2005 as follows:

- CLIN 2003 (CPAF Labor) total funding is decreased by \$493.00 from \$51,089,212.00 to \$51,088,719.00
  - CLIN 2003 funded cost is decreased by \$457.00 from \$47,304,826.00 to \$47,304,369.00
  - CLIN 2003 funded award fee is decreased by \$36.00 from \$3,784,386.00 to \$3,784,350.00
- CLIN 2005 (Tools) funding is decreased by \$9,541.00 from \$16,933,669.00 to \$16,924,128.00

2. Attach the Award Fee Determination Package for Award Fee Period 7.

As a result of this modification, page B-10 of the Task Order, Section B.6.1, Incremental Funding Limitation of Government's Obligation, is updated to reflect the new funding amount for the mandatory CLINs.

The Task Order total funding is decreased by \$10,034.00 from \$319,132,862.00 to \$319,122,828.00.

The Task Order ceiling remains unchanged at \$684,688,778.

All changes are noted by the black change bars in the right margin of the conformed TO.

All other terms and conditions remain unchanged.

# **TASK ORDER**

**GSQ0017AJ0079 P00072**

## **Secure Enterprise Network Systems, Services, & Support (SENS3)**

**in support of:**

## **Department of Homeland Security (DHS) Information Technology Services Office (ITSO)**



**Issued to:  
Leidos, Inc.**

**Awarded under GSA Alliant Government-wide  
Acquisition Contract GS00Q09BGD0039**

**Conducted under Federal Acquisition Regulation (FAR) 16.505**

**Issued by:  
The Federal Systems Integration and Management Center (FEDSIM)  
1800 F Street, NW (QF0B)  
Washington, D.C. 20405**

**August 31, 2017**

**FEDSIM Project Number: HS00800**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### **B.1 GENERAL**

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in Section J, Attachment B.

### **B.2 CONTRACT ACCESS FEE (CAF)**

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. For GSA-issued TOs, the CAF shall be 0.75 percent of the total TO value with a cap of \$100,000 per year per order (when order is in excess of \$13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

### **B.3 ORDER TYPES**

The contractor shall perform the effort required by this TO on a Firm-Fixed Price (FFP) basis for CLINs 0001a, 0001b, 1001, 2001, 3001, 4001, and 5001 and on a Cost-Plus Award Fee basis for CLINs 0002, 0003, 0008, 0009, 1003, 2003, 3003, 4003, and 5003 and on a Not-to-Exceed basis for CLINs 0004, 0005, 0006, 0007, 0010, 0011, 0012, 1004, 1005, 1006, 1007, 2004, 2005, 2006, 2007, 3004, 3005, 3006, 3007, 4004, 4005, 4006, 4007, 5004, 5005, 5006, and 5007. The work shall be performed in accordance with all Sections of this TO and the offeror's Basic Contract, under which the resulting TO will be placed.

#### **B.3.1 ORDER TYPE CHANGE**

Transition from Cost-Plus Award Fee to Firm-Fixed Price (FFP) basis for CLINs 1003, 2003, 3003, 4003, and 5003 will be considered post-award. The Government reserves the right to change contract type to FFP for existing CLINs post-award to allow pricing type changes in pursuit of transitioning individual functional tasks to a managed service.

### **B.4 SERVICES AND PRICES/COSTS**

Long-distance travel is defined as travel over 50 miles from the primary place of performance. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
FFP	Firm-Fixed-Price
NSP	Not Separately Priced
NTE	Not-to-Exceed
ODC	Other Direct Cost
QTY	Quantity

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.1 BASE PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
0001a	Labor (Objective C.4.1) (Transition-In)	(b)(4)		(b)(4)
0001b	Labor (Objective C.4.1)			

CLIN	Description	Cost	Award Fee	Total CPAF
0002	Labor (Objective C.4.2)	(b)(4)		(b)(4)
0003	Labor (Objectives C.4.3 and C.4.4)			

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
0004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500,000
0005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
0006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 14,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
0007	Contract Access Fee	NTE	\$100,000

**TOTAL BASE PERIOD MANDATORY SEVERABLE CLINs:**

(b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.2 FIRST OPTION PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
1001	Labor (Objective C.4.1)	(b)(4)		(b)(4)

CLIN	Description	Cost	Award Fee	Total CPAF
1003	Labor (Objectives C.4.3 and C.4.4)	(b)(4)		(b)(4)

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
1004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500,000
1005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
1006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 14,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
1007	Contract Access Fee	NTE	\$100,000

**TOTAL FIRST OPTION PERIOD MANDATORY SEVERABLE CLINs:** (b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.3 SECOND OPTION PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
2001	Labor (Objective C.4.1)	(b)(4)		(b)(4)

CLIN	Description	Cost	Award Fee	Total CPAF
2003	Labor (Objectives C.4.3 and C.4.4)	(b)(4)		(b)(4)

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
2004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500,000
2005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
2006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 4,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
2007	Contract Access Fee	NTE	\$100,000

**TOTAL SECOND OPTION PERIOD MANDATORY SEVERABLE CLINs:** (b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.4 THIRD OPTION PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
3001	Labor (Objective C.4.1)	(b)(4)		(b)(4)

CLIN	Description	Cost	Award Fee	Total CPAF
3003	Labor (Objectives C.4.3 and C.4.4)	(b)(4)		(b)(4)

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
3004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500,000
3005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
3006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 14,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
3007	Contract Access Fee	NTE	\$100,000

**TOTAL THIRD OPTION PERIOD MANDATORY SEVERABLE CLINs:** (b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.5 FOURTH OPTION PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
4001	Labor (Objective C.4.1)	(b)(4)		

CLIN	Description	Cost	Award Fee	Total CPAF
4003	Labor (Objectives C.4.3 and C.4.4)	(b)(4)		

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
4004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500,000
4005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
4006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 14,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
4007	Contract Access Fee	NTE	\$100,000

**TOTAL FOURTH OPTION PERIOD MANDATORY SEVERABLE CLINs:** (b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**B.4.6 FIFTH OPTION PERIOD:**

**MANDATORY SEVERABLE LABOR CLINs**

CLIN	Description	QTY	Unit	Total FFP
5001	Labor (Objective C.4.1)	(b)(4)		

CLIN	Description	Cost	Award Fee	Total CPAF
5003	Labor (Objectives C.4.3 and C.4.4)	(b)(4)		

**COST REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs**

CLIN	Description		Total NTE Price
5004	Long-Distance Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 1,500, 000
5005	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 20,000,000
5006	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 14,000,000

**CONTRACT ACCESS FEE**

CLIN	Description		Total Ceiling Price
5007	Contract Access Fee	NTE	\$100,000

**TOTAL FIFTH OPTION PERIOD MANDATORY SEVERABLE CLINs:** (b)(4)

**TOTAL ALL MANDATORY SEVERABLE CLINs:**

(b)(4)

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### **B.4.7 OPTIONAL SEVERABLE LABOR CLIN**

CLIN	Description	Cost	Award Fee	Total CPAF
0008	Labor (Objective C.4.5)	(b)(4)		

**TOTAL OPTIONAL SEVERABLE CLIN:**

(b)(4)

### **B.4.8 NONSEVERABLE CLINS**

CLINs 0009, 0010, 0011, and 0012 are for service lifecycle projects and continual service improvement projects (Objectives C.4.3e, C.4.4d, and C.4.4e) that are determined to be non-severable in nature. The labor for each project determined to be non-severable under Objectives C.4.3e, C.4.4d, and C.4.4e is a single undertaking on behalf of participating Federal Agencies, entire in nature, and cannot be feasibly subdivided into discrete elements or phases without losing its integrity and failing to provide the support to plan, document, and execute deployments and improvements of the SENS3. CLINs 0009, 0010, 0011, and 0012 are non-severable. As non-severable projects are identified, the Government will conduct an independent assessment to ensure that the projects meet the criteria for non-severability as established in statute, regulation, and policy. Once a project has been determined by the Government to be non-severable, the Government will modify the TO to create a discrete set of sub-CLINs and associate them with the non-severable project. Each project identified will have its own set of sub-CLINs, and the total ceiling of the sub-CLINs will not exceed the ceiling value of parent CLINs (i.e., 0009, 0010, 0011, and 0012). The SENS3 Database Extract, to be provided with each task order modification and, if applicable with supplemental Excel spreadsheets, tracks each sub-CLINs' estimated costs and applicable fees, project start date, estimated schedule completion date, and the amount of funding available for each approved non-severable project and its preceding Rough Order of Magnitude (ROM), if applicable. In addition, Section J, Attachment C – Incremental Funding Chart (Excel Spreadsheet) will provide the total funding that is allotted and available for CLINs 0009, 0010, 0011, and 0012 and display the appropriate distribution for cost and fee. Non-severable project sub-CLINs shall be fully funded at time of obligation and cannot be incrementally funded.

### **CPAF NONSEVERABLE LABOR CLIN (Optional)**

CLIN	Description	Estimated Cost	Estimated Award Fee	Total Estimated CPAF
0009	Labor (Objectives C.4.3e, C.4.4d, and C.4.4e, upon determination of non-severability)	(b)(4)		(b)(4)

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

**COST REIMBURSABLE NONSEVERABLE TRAVEL, TOOLS, and ODC CLINs  
(Optional)**

CLIN	Description		Total Ceiling Price
0010	Travel Including Indirect Handling Rate (b)(4)	NTE	\$ 6,000,000
0011	Tools Including Indirect Handling Rate (b)(4)	NTE	\$ 120,000,000
0012	ODCs Including Indirect Handling Rate (b)(4)	NTE	\$ 6,000,000

**TOTAL ALL NON-SEVERABLE CLINs:**

(b)(4)

**GRAND TOTAL ALL CLINs:**

**\$684,688,778**

## **B.5 SECTION B TABLES**

### **B.5.1 INDIRECT/MATERIAL HANDLING RATE**

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

- a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
- b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

### **B.5.2 DIRECT LABOR RATES**

Labor categories proposed shall be mapped to existing Alliant labor categories.

## **B.6 INCREMENTAL FUNDING**

### **B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION**

Incremental funding in the amount of **\$308,909,296** for CLINs **0001a, 0001b, 0002, 0003, 0004, 0005, 0006, 0007, 0009, 0010, 0011, 0012, 100,1, 1003, 1004, 1005, 1006, 1007, 2001, 2003, 2004, 2005, 2006, 2007, 3001, 3003, 3004, 3005, 3006, and 3007** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **August 30, 2021** unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of **\$684,688,778** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

#### **Incremental Funding Chart for CPAF**

See Section J, Attachment C - Incremental Funding Chart (Excel Spreadsheet).

### **B.7 AWARD FEE PLANNED VALUE/RESULTS REPORTING TABLE**

The Award Fee Determination Plan (AFDP) establishes award fee. See Section J, Attachment D – Award Fee Determination Plan (Word document).

## SECTION C – STATEMENT OF OBJECTIVES

### **C.1 BACKGROUND**

#### **C.1.1 PURPOSE**

The Department of Homeland Security's (DHS) Information Technology Services Office (ITSO) and Office of Intelligence & Analysis (I&A) have a requirement for Secure Enterprise Network Systems, Services, & Support (SENS3) to address the mission-critical need for DHS to maintain and manage effective secure classified information sharing and safeguarding of classified information among all DHS Components, its Federal, state, local, and tribal partners, and stakeholders in support of its classified enterprise operations. The DHS mission is dependent on a secure, reliable, and capable classified information sharing infrastructure that is interoperable across DHS and partner classified environments. These environments consist of the Homeland Secure Data Network (HSDN), the C-LAN, and supporting systems and interfaces, as well as cross domain guards connecting the DHS unclassified networks with HSDN and C-LAN networks. DHS was specifically directed to address these requirements through multiple legislative actions and executive orders including, but not limited to: the Homeland Security Act of 2002, as amended; the Implementing the Recommendations of the 9-11 Commission Act of 2007, Executive Order (EO) 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans;" and EO 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

The HSDN is the Secret-level, civilian classified network with connectivity to the Defense Information System Agency (DISA) provisioned Secret Internet Protocol Router Network (SIPRNet). The C-LAN provides similar services at the Top Secret/Sensitive Compartmented Information (TS/SCI) level with connectivity to the Defense Intelligence Agency (DIA)-provisioned Joint Worldwide Intelligence Communications System (JWICS). These DHS classified networks provide a Federal enterprise infrastructure for classified information sharing that extends existing United States (U.S.) Government capabilities not only to DHS, but to other Federal Government agencies and to first responders at the state, local, and tribal levels.

The continued evolution of the HSDN and the C-LAN will leverage advancements in technology to enhance or replace existing network components with newer, better maintained technologies to avoid performance degradation and obsolescence. This continual service improvement includes the formulation and the execution of alternative approaches and architectures for optimizing and modernizing the HSDN and the C-LAN networking environments, including managed service models and available cloud technologies.

#### **C.1.2 AGENCY MISSION**

DHS is a widely distributed and diverse national enterprise. The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. These concepts have led DHS to define its core mission set as:

- a. Preventing Terrorism and Enhancing Security,
- b. Securing and Managing Our Borders,
- c. Enforcing and Administering Our Immigration Laws,
- d. Safeguarding and Securing Cyberspace,

## SECTION C – STATEMENT OF OBJECTIVES

- e. Ensuring Resilience to Disasters.

### **C.2 SCOPE**

The scope of SENS3 addresses the operations and maintenance, security, optimization, enhancement, design, engineering, architecture, integration, configuration, testing, and deployment of the DHS HSDN and C-LAN networks, infrastructure (including hardware and software), cross domain services operating on DHS unclassified, HSDN and C-LAN networks, and other systems supporting the intelligence mission collectively referred to as the SENS3 networks (see Section J, Attachment E – Functional Requirements).

### **C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT**

The network infrastructure environment managed by DHS is used to deliver secure enterprise network systems and services. When the Department was stood up in 2003, the infrastructure it inherited comprised dozens of networks that had earlier been developed and managed independently by the previously separate agencies. Under “One DHS” policies, the DHS Office of the Chief Information Officer (OCIO) has been merging and harmonizing existing networks into offerings that will provide effective and efficient network services, while saving considerable costs through a common architecture, shared management, and leveraged investments. Central to the infrastructure transformation program is the separate OneNet initiative. OneNet comprises network circuit provisioning orders established under the GSA Networkx program to supply DHS with its communications connectivity. DHS currently operates one unclassified network (A-LAN) and two secure, classified networks, HSDN which operates at the Secret level and C-LAN which operates at the TS/SCI level. HSDN and the C-LAN provide a common core of essential services (e.g., Service Desk, Network Operations Center (NOC), cross-domain services, servers, and virtual machines) and the associated infrastructure, which are necessary to operate and maintain the IT environments for all users. SENS3 also includes support for other systems supporting the intelligence mission (see Section J, Attachment E – Functional Requirements).

The HSDN is a fully operational Government-wide infrastructure solution managed by DHS, designed and implemented to provide standardized, secure transport with desktop applications to enable a consistent classified capability in support of the DHS mission. HSDN is deployed to more than 700 locations across the continental U.S. including many locations at other Federal agencies and over 40 SLFCs (see Section J, Attachment FF – HSDN and C-LAN Site Deployment Map). It is isolated from the Internet with no public access. HSDN has approval to operate in accordance with DHS Policy 4300B, which is based upon Committee on National Security Systems instruction (CNSSI) 1253, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) and NIST SP 800-53A (Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations) security standards. HSDN consists of two sets of fully redundant core infrastructures of routers, servers, and data storage located at the two DHS Data Centers (DC1 and DC2) and connected by DHS’ wide area network (OneNet) that carries only classified network traffic in an encrypted state. It also includes two redundant gateways connecting HSDN as a peer to other Secret networks (e.g., the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNet)), a NOC, Public Key Infrastructure (PKI), and a service desk. The HSDN core infrastructure connects to end-user sites via DHS OneNet as a backbone network. Networked components at those nodes include end

## SECTION C – STATEMENT OF OBJECTIVES

point routers, encryptors, thick clients, thin clients, printers, Secure Video Teleconferencing (SVTC) clients, and voice over secure internet protocol (VoSIP) clients. Services hosted on the HSDN core infrastructure include electronic mail (email), organizational messaging (e.g., the Automated Message Handling System (AMHS)), SVTC connection and bridging, a web portal, collaboration tools, application hosting services, global backup and recovery services, and standard office productivity tools. The HSDN core infrastructure connects to handheld devices for secret-level voice capability through a mobile architecture accepted by the Commercial Solutions for Classified (CSfC) Program. HSDN offers several standard end-point configurations including handheld devices, laptops, small sites, medium sites, and large custom sites.

C-LAN is a fully operational DHS enterprise-wide infrastructure solution designed and implemented to provide standardized, secure transport with desktop applications to enable a consistent TS/SCI capability in support of the DHS mission. C-LAN is deployed to more than 50 locations across the continental U.S. including state and local partners (see Section J, Attachment FF – HSDN and C-LAN Site Deployment Map). It is isolated from the Internet with no public access. C-LAN has approval to operate in accordance with DHS Policy 4300C. C-LAN consists of two sets of fully redundant core infrastructures of routers, servers, and data storage located at DC1 and DC2 and connected by DHS' wide area network (OneNet). C-LAN provides a NOC, a Voice/Video Operations Center (VVOC), and a service desk as an enclave of JWICS. The C-LAN core infrastructure connects to end-user sites via DHS OneNet as a backbone network. Networked components at those nodes include end point routers, encryptors, thick clients, thin clients, printers, SVTC clients, and VoSIP clients. Services hosted on the C-LAN core infrastructure include electronic mail (email), organizational messaging (e.g., AMHS), SVTC connection and bridging, a web portal, collaboration tools, application hosting services, global backup and recovery services, and standard office productivity tools.

### **C.4 OBJECTIVES**

The objectives for SENS3 represent the desired outcomes of the support services being sought with an overall objective of no degradation to the current functional requirements. The current functional requirements of SENS3 are detailed in Section J, Attachment E – Functional Requirements. Offerors are challenged to provide innovative and cost-effective technical, management, and staffing approaches that meet the following objectives.

#### **C.4.1 MANAGE TASK ORDER**

- a. Provide management, direction, administration, quality control, and leadership of the execution of this TO in accordance with Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) and Information Technology Infrastructure Library (ITIL) best practices or comparable IT services management (ITSM) framework.
- b. Provide effective and transparent communications in performing all work and when addressing issues.
- c. Provide a web-based collaborative SENS3 project portal to include functionality for a document library, managing site deployment requests, and a dashboard of the infrastructure status (e.g., key events, incidents, and performance statistics). Distinct but similarly structured and linked portals are required for SENS3 overall (Unclassified), HSDN-specific activities (hosted on HSDN), and C-LAN-specific activities (hosted on

## SECTION C – STATEMENT OF OBJECTIVES

C-LAN). The tool shall be accessible to authorized personnel in DHS, Other Government Agencies (OGAs), and state, local, and tribal partners.

- d. Monitor, document, report, and improve management, direction, administration, quality control, and leadership of the execution of this TO.

### **C.4.2 SENS3 TRANSITION-IN**

- a. Coordinate and integrate transition activities with the incumbent contractor during a 120-day transition in of SENS3.
- b. Coordinate and integrate transition activities with other enterprise service providers.
- c. Coordinate and integrate transition activities with users and stakeholders of SENS3.
- d. Create a transition-in plan that incorporates the DHS suitability determination process (Entry on Duty (EOD)).
- e. Transition the current environment with minimal to no service disruption (see Section J, Attachment Z - Current Service Level Agreements).

### **C.4.3 SENS3 SERVICE LIFECYCLE**

- a. Operate and maintain the SENS3 networks in accordance with the Government-approved PWS, Government-approved Service Level Agreements (SLAs), and security policies.
- b. Coordinate activities with Government organizations and their contractors responsible for systems that have connectivity with DHS assets within the scope of SENS3 (see Section J, Attachment QQ - Interactions with Other Service Providers).
- c. Ensure minimal to no service disruption to the SENS3 networks.
- d. Monitor, document, report, and improve the user experience (e.g., service delivery timeline, transparency, self-service options) and service lifecycle planning, implementation, performance, and control.
- e. Plan, document, and implement projects (e.g., sites deployments, network migrations, and temporary secure facilities) providing costs, schedule, and status for all projects.

### **C.4.4 SENS3 CONTINUAL SERVICE IMPROVEMENT (CSI)**

- a. Provide planning and recommendations for continual improvement of the SENS3 networks to meet or exceed mission-enablement and operational effectiveness and efficiency goals.
- b. Research, recommend, and utilize the best of commercially available IT technologies.
- c. Improve the user experience.
- d. Leverage and coordinate transitions to Intelligence Community Information Technology Enterprise (IC ITE) services with IC ITE services providers and their contractors (see Section J, Attachment J – Notional IC ITE Transition Roadmap).
- e. Provide implementation of CSI projects with minimal to no service disruption to the SENS3 networks.
- f. Monitor, document, report, and improve CSI planning, implementation, performance, and control.

## SECTION C – STATEMENT OF OBJECTIVES

### **C.4.5 SENS3 TRANSITION-OUT**

- a. Coordinate and integrate transition activities with the incoming contractor during a 120-day transition-out of SENS3.
- b. Coordinate and integrate transition activities with other enterprise service providers.
- c. Coordinate and integrate transition activities with users and stakeholders of SENS3.
- d. Maintain minimal to no service disruption to the SENS3 networks during transition-out of SENS3.

### **C.5 CONSTRAINTS**

#### **C.5.1 POLICIES, DIRECTIVES, AND STANDARDS**

Existing policies, directives, and standards that are constraining factors for SENS3 requirements include, but are not limited to:

- a. DHS Policy 4300B
- b. DHS Policy 4300C
- c. Committee on National Security Systems Policies (CNSSP) No. 11, “National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products.”

#### **C.5.2 FUNDING/APPROPRIATIONS**

- a. The SENS3 funding environment is complex. HSDN receives annual congressional appropriations to support the Department’s homeland security mission, as well as State and Local Fusion Centers (SLFCs). C-LAN utilizes a working capital fund. Projects are funded by over twenty different customer agencies. Funds have varying expiration dates (e.g. 1-year, multi-year, and no-year) and must often be reviewed and approved by customer agencies’ funding offices before being sent to GSA and added to the contract. This complexity can lead to delays between the final cost estimate for a project and the availability of funding for the contractor to begin the project.

SECTION D - PACKAGING AND MARKING

This page intentionally left blank.

## SECTION E - INSPECTION AND ACCEPTANCE

### **E.1 PLACE OF INSPECTION AND ACCEPTANCE**

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) in the Washington, D.C., metropolitan area.

### **E.2 SCOPE OF INSPECTION**

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and DHS TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

### **E.3 BASIS OF ACCEPTANCE**

The basis for acceptance shall be in compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

### **E.4 DRAFT DELIVERABLES**

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

## SECTION E - INSPECTION AND ACCEPTANCE

### **E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT**

The FEDSIM CO/COR will provide written notification of acceptance or rejection (Section J, Attachment I) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

### **E.6 NON-CONFORMING PRODUCTS OR SERVICES**

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

For FFP -

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will withhold the fixed price until the non-conforming products or services are remediated.

For CPAF –

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the award fee earned.

## SECTION F – DELIVERABLES OR PERFORMANCE

### **F.1 PERIOD OF PERFORMANCE**

The period of performance for severable CLINs under this TO is a one-year base period and five, one-year option periods.

The period of performance for each non-severable project under this TO will be identified in SENS3 Database Extract. The completion date for any individual non-severable project shall not exceed the total period of performance for the TO.

### **F.2 PLACE OF PERFORMANCE**

The primary place of performance shall be at the contractor's facility. In addition to office space, the contractor's facility shall include spaces suitable for a development and test facility and classified IT storage. The contractor facility shall be accreditable to TS/SCI.

For O&M on-site support, a total of 32 seats will initially be provided by the Government at various locations in the National Capital Region and other DHS facilities supported under this TO (e.g., DC1). All of the remaining effort under this TO will be performed at the contractor site and through long-distance travel.

Other places of performance for on-site work, based on the operational situation at any point in time, shall occur at any HSDN or C-LAN infrastructure location, such as DC1 (Mississippi) and DC2 (Virginia), and at any end-user location (any HSDN or any C-LAN site). Sites are located all over the U.S. and territories (Section J, Attachment FF and Attachment KK). Future DHS plans may include selected foreign countries.

Long-distance travel shall be required in support of this effort. For the purposes of this task order, determination of long distance travel is dependent upon an individual contractor employee's duty location.

### **F.3 TASK ORDER SCHEDULE AND MILESTONE DATES**

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable

IAW: In Accordance With

NLT: No Later Than

TOA: Task Order Award

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

<b>DEL. #</b>	<b>MILESTONE/ DELIVERABLE</b>	<b>CLIN</b>	<b>TOR REFERENCE</b>	<b>DATE OF COMPLETION/ DELIVERY</b>	<b>GOV'T RIGHTS</b>
01	Project Start (PS)	0001a	C.4.1	At TOA plus 10 days	

SECTION F – DELIVERABLES OR PERFORMANCE

<b>DEL. #</b>	<b>MILESTONE/ DELIVERABLE</b>	<b>CLIN</b>	<b>TOR REFERENCE</b>	<b>DATE OF COMPLETION/ DELIVERY</b>	<b>GOV'T RIGHTS</b>
02	Kick-Off Meeting Agenda	0001a	C.4.1	At least three days prior to the Kick-Off Meeting	Unlimited IAW 52.227- 14(c)(1)
03	Kick-Off Meeting	0001a	C.4.1	Within 5 days of PS	
04	Draft Performance Work Statement (PWS)	0001a	C.4.1	Within 5 days of PS	Unlimited IAW 52.227- 14(c)(1)
05	Finalize PWS	0001a	C.4.1	Within 30 days of PS	Unlimited IAW 52.227- 14(c)(1)
06	PWS Revisions	0001b	C.4.1, F.3.1	Biannually	Unlimited IAW 52.227- 14(c)(1)
07	Draft Service Level Agreements (SLAs)	0001a	C.4.1	Within 5 days of PS	Unlimited IAW 52.227- 14(c)(1)
08	Finalize SLAs	0001a	C.4.1	December 1, 2017	Unlimited IAW 52.227- 14(c)(1)
09	SLA Revisions	0001b	C.4.1, F.3.2	Biannually	Unlimited IAW 52.227- 14(c)(1)
10	Integrated Master Schedule (IMS)	0001a, 0001b	C.4.1	Within 5 days of PS	Unlimited IAW 52.227- 14(c)(1)
11	Updated IMS	0001a, 0001b	C.4.1	Offeror Propose	Unlimited IAW 52.227- 14(c)(1)
12	Monthly Status Report	0001a, 0001b	C.4.1	Monthly 10 <sup>th</sup> calendar day of the next month	Unlimited IAW 52.227- 14(c)(1)
13	Draft Project Management Plan (including Quality Assurance Plan)	0001a	C.4.1	Due at Kick-Off Meeting	Unlimited IAW 52.227- 14(c)(1)
14	Final Project Management Plan (including Quality Assurance Plan)	0001a	C.4.1	10 workdays after receipt of Government comments	Unlimited IAW 52.227- 14(c)(1)
15	Project Management Plan Updates (including Quality Assurance Plan)	0001a, 0001b	C.4.1	As project changes occur, no less frequently than annually	Unlimited IAW 52.227- 14(c)(1)

## SECTION F – DELIVERABLES OR PERFORMANCE

<b>DEL. #</b>	<b>MILESTONE/ DELIVERABLE</b>	<b>CLIN</b>	<b>TOR REFERENCE</b>	<b>DATE OF COMPLETION/ DELIVERY</b>	<b>GOV'T RIGHTS</b>
16	Acquisition Risk Questions	0001a	H.16	Submitted with Quote; Update at Kick-Off Meeting	Unlimited IAW 52.227-14(c)(1)
17	Updated Transition-In Plan	0001a	C.4.1	Due at Kick-Off Meeting	Unlimited IAW 52.227-14(c)(1)
18	Final Transition-In Plan	0001a	C.4.1	10 workdays after receipt of Government comments	Unlimited IAW 52.227-14(c)(1)
19	Draft Transition-Out Plan	0001b	C.4.1	Within six months of Project Start	Unlimited IAW 52.227-14(c)(1)
20	Final Transition-Out Plan	0001b	C.4.1	10 workdays after receipt of Government comments	Unlimited IAW 52.227-14(c)(1)

**The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.**

### **F.3.1 PERFORMANCE WORK STATEMENT (PWS)**

The contractor's PWS will be incorporated as an attachment in Section J of the TO. At a minimum, the contractor shall submit a revised PWS twice a year. Any revisions made shall be consistent with implementing the objectives in Section C, Statement of Objectives (SOO), and reflect the most current operational environment of the SENS3 networks. The Government will review any revisions and unilaterally determine if they are acceptable.

### **F.3.2 SERVICE LEVEL AGREEMENTS (SLAs)**

The contractor's SLAs will be incorporated as an attachment in Section J of the TO. At a minimum, the contractor shall submit revised SLAs twice a year. Any revisions made shall be consistent with implementing the objectives in Section C, Statement of Objectives (SOO), and reflect the most current operational environment of the SENS3 networks. The Government will review any revisions and unilaterally determine if they are acceptable.

### **F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT**

The contractor agrees to submit, within five workdays from the date of the FEDSIM CO's request (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be

## SECTION F – DELIVERABLES OR PERFORMANCE

privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

### **F.5 DELIVERABLES MEDIA**

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in DHS's designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- |                 |               |
|-----------------|---------------|
| a. Text         | MS Word       |
| b. Spreadsheets | MS Excel      |
| c. Briefings    | MS PowerPoint |
| d. Drawings     | MS Visio      |
| e. Schedules    | MS Project    |

### **F.6 PLACE(S) OF DELIVERY**

Copies of all deliverables shall be delivered to the FEDSIM COR or Alternate COR (ACOR) at the following address:

GSA FAS AAS FEDSIM  
ATTN: TJ Chen, COR (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 969-4097  
Email: tj.chen@gsa.gov

GSA FAS AAS FEDSIM  
ATTN: Tim Eicher, ACOR (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 288-9516  
Email: timothy.eicher@gsa.gov

Copies of all deliverables shall also be delivered to the DHS TPOC. The TPOC name, address, and contact information will be provided at award.

**F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)**

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (Section J, Attachment F) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

**G.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR)**

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (Section J, Attachment A). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

**G.1.1 CONTRACT ADMINISTRATION**

Contracting Officer:

Nydia Roman-Albertorio  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 285-9530  
Email: nydia.roman-albertorio@gsa.gov

Contracting Officer’s Representative:

TJ Chen  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 969-4097  
Email: tj.chen@gsa.gov

Alternate Contracting Officer’s Representative:

Tim Eicher  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 288-9516  
Email: timothy.eicher@gsa.gov

Technical Points of Contact:

HSDN:

Oliver Clark  
DHS OCIO  
245 Murray Lane  
Washington, DC 20528-0001  
Telephone: 202.357.8445

## SECTION G – CONTRACT ADMINISTRATION DATA

Email: [oliver.clark@hq.dhs.gov](mailto:oliver.clark@hq.dhs.gov)

C-LAN:

Primary Point of Contact:

Robert McDermott

DHS I&A OCIO

245 Murray Lane

Washington, DC 20528-0001

Telephone: 228-813-3305 (UNCLASS)

Telephone: 202-878-2852 (CELL)

Email: [robert.mcdermott.2@hq.dhs.gov](mailto:robert.mcdermott.2@hq.dhs.gov)

### **G.2 INVOICE SUBMISSION**

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*

FEDSIM Project Number: HS00800

Project Title: Secure Enterprise Network Systems, Services, and Support (SENS3)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

<https://portal.fas.gsa.gov>

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. The AASBS Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at [AASBS.helpdesk@gsa.gov](mailto:AASBS.helpdesk@gsa.gov). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

### **G.3 INVOICE REQUIREMENTS**

The contractor shall submit a draft copy of an invoice to GSA and the Technical Point of Contact (TPOC) for review prior to its submission to GSA. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. The contractor shall submit simultaneous copies of the invoice to both GSA and the TPOC. Receipts are provided on an as requested basis.

If the TO has different contract types, each should be addressed separately in the invoice submission.

If the TO has severable and non-severable cost CLINs, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following:

- a. GWAC Contract Number
- b. Task Order Award Number (NOT the Solicitation Number)
- c. Contractor Invoice Number
- d. Current period of performance.
- e. Amount of invoice that was subcontracted.
- f. Amount of invoice that was subcontracted to a small business.

#### **G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)**

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- a. Employee name (current and past employees)
- b. Employee company
- c. Employee Alliant labor category
- d. Exempt or non-exempt
- e. Monthly and total cumulative hours worked
- f.
- g. Effective hourly rate
- h. Any cost incurred not billed
- i. Labor adjustments (from any previous months (e.g., timesheet corrections))
- j. Current approved billing rates in support of costs billed
- k. Project reference number

## SECTION G – CONTRACT ADMINISTRATION DATA

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges at a minimum at the cost center level and shall also include the Overhead and General and Administrative rates being applied.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP in Section J, Attachment D for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

### **G.3.2 FIRM-FIXED-PRICE (FFP) CLINs**

The contractor may invoice as stated in Section B for the FFP CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All prices shall be reported by CLIN element (as shown in Section B) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- a. FFP period of performance – as stated in Section B
- b. Total Amount Paid (Lump Sum) by CLIN

### **G.3.3 TOOLS AND OTHER DIRECT COSTS (ODCs)**

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- a. Tools and/or ODCs purchased
- b. Request for Change (RFC) or Consent to Purchase (CTP) number or identifier
- c. Date accepted by the Government
- d. Associated CLIN
- e. Project-to-date totals by CLIN
- f. Cost incurred not billed
- g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead charges, General and Administrative charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

### **G.3.4 TRAVEL**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Joint Travel Regulation (JTR) - prescribed by the GSA, for travel in the contiguous U.S.

## SECTION G – CONTRACT ADMINISTRATION DATA

- b. Federal Travel Regulation (FTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas” - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period’s travel details shall include separate columns and totals and include the following:

- a. Travel Authorization Request number or identifier, approver name, and approval date
- b. Current invoice period
- c. Names of persons traveling
- d. Number of travel days
- e. Dates of travel
- f. Number of days per diem charged
- g. Per diem rate used
- h. Total per diem charged
- i. Transportation costs
- j. Total charges
- k. Explanation of variances exceeding ten percent of the approved versus actual costs
- l. Indirect handling rate

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges in accordance with the contractor’s DCAA cost disclosure statement.

### **G.4 TASK ORDER CLOSEOUT**

The Government will unilaterally close out the TO six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

## **H.1 KEY PERSONNEL**

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this TO. The offeror shall propose appropriate labor categories for these positions.

- a. Project Manager
- b. Chief Engineer/Architect
- c. HSDN Manager
- d. C-LAN Manager
- e. Operations Manager

The Government desires that Key Personnel be assigned for the duration of the TO.

### **H.1.1 PROJECT MANAGER (PM)**

The contractor shall provide a PM to serve as the contractor's single TO manager and shall be the contractor's authorized interface with the FEDSIM CO, FEDSIM COR, and TPOC for the TO. The PM shall be responsible for overall TO performance. The PM shall be available to plan, direct, and control the overall management and operational functions specified herein during normal hours of operation, and during periods of no-notice emergencies, including localized acts of nature, accidents, and military or terrorist attacks.

It is desired that the PM has the following qualifications:

- a. Certification in Project Management from a recognized credentialing agency (e.g., Project Management Professional (PMP) from the Project Management Institute (PMI)).
- b. A Bachelor's degree in IT, Computer Science, Information Systems, or related field.
- c. Experience organizing, directing, and managing contract operation support functions involving multiple, complex, and interrelated project tasks.
- d. Experience effectively communicating at senior levels within a customer organization.
- e. Experience meeting with customer and contractor personnel to formulate and review task plans and deliverable items, and effectively execute in accordance with approved plans.
- f. Experience managing tools and purchases and a demonstrated understanding of purchasing systems.

### **H.1.2 CHIEF ENGINEER/ARCHITECT**

The contractor shall provide a Chief Engineer/Architect to direct the engineering team in the architecture and design of solutions to meet requirements and improve service.

It is desired that the Chief Architect have the following qualifications:

- a. Certification in security practices such as a Certified Information Systems Security Professional (CISSP).
- b. A Bachelor's degree in IT, Computer Science, Information Systems, or related field.
- c. At least five years of experience with engineering/architecting secured enterprise IT solutions.
- d. Experience with engineering/architecting secured enterprise telecommunication solutions.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- e. Experience providing detailed engineering and technical leadership to engineering staff involving multiple, complex, and interrelated project tasks.
- f. Experience effectively communicating at senior levels within a customer organization.

### **H.1.3 HSDN MANAGER**

The contractor shall provide an HSDN Manager who is responsible for all activities required to operate, maintain, and continually improve HSDN. The HSDN Manager shall manage and provide oversight of all activities performed by contractor personnel to satisfy the HSDN requirements identified in the contract.

It is desirable that the HSDN Manager have the following qualifications:

- a. A Bachelor's degree in IT, Computer Science, Information Systems, or related field.
- b. Certification in Project Management from a recognized credentialing agency (e.g., PMP from the PMI).
- c. Experience organizing, directing, and managing operations and maintenance support functions involving multiple, complex, and interrelated project tasks.
- d. Experience providing detailed technical leadership to staff involving multiple, complex, and interrelated project tasks.

### **H.1.4 C-LAN MANAGER**

The contractor shall provide a C-LAN Manager who is responsible for all activities required to operate, maintain, and continually improve C-LAN. The C-LAN Manager shall manage and provide oversight of all activities performed by contractor personnel to satisfy the C-LAN requirements identified in the contract

It is desirable that the C-LAN Manager have the following qualifications:

- a. A Bachelor's degree in IT, Computer Science, Information Systems, or related field.
- b. Certification in Project Management from a recognized credentialing agency (e.g., PMP from the PMI).
- c. Experience organizing, directing, and managing operations and maintenance support functions involving multiple, complex, and interrelated project tasks.
- d. Experience providing detailed technical leadership to staff involving multiple, complex, and interrelated project tasks.

### **H.1.5 OPERATIONS MANAGER**

The contractor shall provide an Operations Manager to assume overall responsibility with respect to the execution of the SENS3 Service Lifecycle.

It is desirable that the Operations Manager have the following qualifications:

- a. A Bachelor's degree in IT Systems Management or equivalent.
- b. At least five years of demonstrated experience in the successful IT operations and management of all aspects of maintaining classified enterprise IT and telecommunication services at customer and other infrastructure locations.
- c. Working knowledge of managing classified enterprise IT and telecommunication asset inventories.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- d. Working knowledge of managing classified enterprise IT and telecommunication operation and maintenance services (e.g., Service Desk, Deskside Support, NOC, PKI Registration Authority, COMSEC material custody,).
- e. Working knowledge of managing and maintaining the IT and telecommunication lifecycles; replacement of hardware and software and the management of consumables and sparing inventories.
- f. Experience in ensuring SLA compliance.

### **H.1.6 KEY PERSONNEL SUBSTITUTION**

The contractor shall not replace any personnel designated as key personnel without the written concurrence of the FEDSIM CO. Prior to utilizing personnel other than those specified in proposals in response to a TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR of the TO. This notification shall be no later than 10 calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

### **H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)**

The Government will provide the workspace, equipment, software, and supplies necessary to perform the on-site portion of contractor services required in this TO, unless specifically stated otherwise in this TO.

For O&M on-site support, a total of 32 seats will initially be provided by the Government at various locations in the National Capital Region and other DHS facilities supported under this TO (e.g., DC1). All of the remaining effort under this TO will be performed at the contractor site and through long-distance travel.

In cases where the Government does not or cannot provide the appropriate workspace, equipment, software, and supplies, the contractor shall provide additional workspaces, equipment, software, and supplies as needed to fulfill the requirements of the TO.

#### **H.2.1 GOVERNMENT-FURNISHED INFORMATION (GFI)**

The contractor shall use GFI, data, and documents only for the performance of work under this TO, and shall be responsible for returning all GFI, data, and documents to the Government at the end of the performance period. The contractor shall not release GFI, data, and documents to outside parties without the prior and explicit consent of the FEDSIM CO.

### **H.3 SECURITY REQUIREMENTS**

Interim clearances are not permitted. All security clearances must be fully adjudicated and approved. At award, all contractor personnel working on HSDN shall possess a minimum of a SECRET level clearance. All contractor personnel working on C-LAN shall possess a fully

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

adjudicated and approved TS/SCI level clearance. It shall be the responsibility of the contractor to initiate reinvestigations of these persons through the Office of Personnel Management (OPM).

All Key Personnel are required to have a current fully adjudicated and approved TS/SCI clearance and access at proposal due date. All personnel working at sites within Sensitive Compartmented Information Facilities (SCIFs), for activities other than installation and periodic maintenance, shall possess a fully adjudicated and approved TS/SCI level clearance and access. The Government anticipates that the number of such personnel could approach 50 percent to 80 percent of the contractor technical personnel over the term of the TO.

COMSEC personnel are required to have a fully adjudicated and approved TS clearance with eligibility for SCI access.

Additional details will be specified in a Department of Defense (DOD) DD Form 254 (Section J, Attachment RR).

### **H.3.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12)**

The contractor shall provide a list of contractor personnel that require DHS badges and security clearances. The Government will process background investigation and/or security clearances for the contractor staff to occur after submission of the staff listing, provided the individuals meet the necessary security qualifications. The Government may grant approved contractor personnel temporary access to the site, subject to compliance with security and safety requirements, within 30 days of TOA. This does not provide access to any DHS accounts, systems, or locations.

### **H.3.2 POST-AWARD SECURITY REQUIREMENTS**

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Contractor employees under the TO, requiring access to sensitive information, shall be able to obtain “DHS Suitability.” The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective contractor employees shall submit the following completed forms to the DHS Office of Security/PSD. The Standard Form (SF) 85P will be completed electronically, through the OPM’s e-QIP System. The completed forms must be given to the DHS Office of Security/PSD no more than three days after date of the TOA or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- a. Standard Form 85P, “Questionnaire for Public Trust Positions”
- b. FD Form 258, “Fingerprint Card” (2 copies)
- c. DHS Form 11000-6 “Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement”
- d. DHS Form 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act”

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of the TO.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the Government do not relieve a contractor from performing under the terms of the TO.

DHS may, as it deems appropriate, authorize and grant a favorable EOD decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information, at any time during the term of the TO. No employee of the contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five days of occurrence. The contractor shall return to the COR all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

DHS Security Office POC Information:

Office of Security/PSD  
Customer Service Support  
Washington, D.C. 20528  
Telephone: (202) 447-5010

### **H.3.3 SECURITY COMPLIANCE REQUIREMENTS**

#### **H.3.3.1 COMPLIANCE WITH DHS SECURITY POLICY**

All sensitive but unclassified (SBU) systems employed by this task must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A *Sensitive Systems Handbook*. All contractor systems used to process sensitive DHS data must be accredited for that use.

All national security systems produced by or supported under this TO must be compliant with DHS 4300B *DHS National Security System Policy*.

All DHS intelligence systems produced by or supported under this TO must be compliant with DHS 4300C *DHS Sensitive Compartmented Information (SCI) Systems Policy Directive*.

### **H.3.3.2 ACCESS TO UNCLASSIFIED FACILITIES, INFORMATION TECHNOLOGY (IT) RESOURCES, AND SENSITIVE INFORMATION**

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and TO performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. The contractor shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all task orders that require access to DHS facilities, IT resources or sensitive information. The contractor shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the TO.

### **H.3.3.3 SECURITY REVIEW**

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this TO are being implemented and enforced. The contractor shall afford DHS, including the organization of DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized FEDSIM COR, and other Government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this TO. The contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of Government oversight organizations external to DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

### **H.3.3.4 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY (IT) RESOURCES**

All unclassified IT resources shall be managed and controlled in compliance with the Department of Homeland Security Acquisition Regulation (HSAR) clause 3004.470: Security requirements for access to unclassified facilities, information technology resources, and sensitive information.

### **H.3.3.5 CONTRACTOR EMPLOYEE ACCESS**

All contractor employee access shall be managed and controlled in compliance with HSAR clause 3004.470: Security requirements for access to unclassified facilities, information technology resources and sensitive information.

### **H.3.3.6 ADDITIONAL INFORMATION FOR CLASSIFIED TASK ORDERS**

All contractor handling of classified information shall be controlled in accordance with the DD Form 254 and comply with the following clauses in accordance with FAR 52.204-2 Security Requirements (Aug 1996).

**H.3.4 DHS SPECIAL CLAUSE - SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)**

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions.* As used in this clause –

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual’s identity, such as name, Social Security Number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

(including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security Numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal history
- (7) Medical information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

- (c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor’s invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component Privacy Officer. Unless otherwise specified in the

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) *Complete the Security Authorization process.* The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

- (i) **Security Authorization Process Documentation.** SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.
- (ii) **Independent Assessment.** Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlines in *NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.
- (iii) **Support the completion of the Privacy Threshold Analysis (PTA) as needed.** As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete the PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about use, access, storage, and maintenance of PII on the

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any email. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

### *(g) Sensitive Information Incident Response Requirements*

- (1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
- (2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
  - (i) Inspections,
  - (ii) Investigations,
  - (iii) Forensic reviews, and
  - (iv) Data analyses and processing.
- (4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

### *(h) Additional PII and/or SPII Notification Requirements*

- (1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
- (2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
  - (i) A brief description of the incident;
  - (ii) A description of the types of PII and SPII involved;
  - (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- (iv) Steps individuals may take to protect themselves;
  - (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
  - (vi) Information identifying who individuals may contact for additional information.
- (i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
  - (1) Provide notification to affected individuals as described above; and/or
  - (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:
    - (i) Triple credit bureau monitoring;
    - (ii) Daily customer service;
    - (iii) Alerts provided to the individual for changes and fraud; and
    - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
  - (3) Establish a dedicated call center. Call center services shall include:
    - (i) A dedicated telephone number to contact customer service within a fixed period;
    - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
    - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
    - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
    - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
    - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.
- (j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

### **H.3.5 DHS SPECIAL CLAUSE - INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

- (a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### *(b) Security Training Requirements.*

- (1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.
- (2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.
- (c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. HSAR Class Deviation 15-01 Attachment 1: Safeguarding of Sensitive Information (MAR 2015) Page 2 of 2 DRAFT Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

### **H.4 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS**

#### **H.4.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)**

- a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
- b. The contractor is required to complete and sign an OCI Statement (Section J, Attachment L). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
- c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
- d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
- e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government and the contractor may be found ineligible for award. Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the United States to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

#### **H.4.2 NON-DISCLOSURE REQUIREMENTS**

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment M) and ensure that

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

- a. Are listed on a signed Addendum to the NDA Form (Section J, Attachment N) prior to the commencement of any work on the TO.
- b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
- c. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

### **H.5 SECTION 508 COMPLIANCE REQUIREMENTS**

Unless the Government invokes an exception, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

### **H.6 COST ACCOUNTING SYSTEM**

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract.

### **H.7 PURCHASING SYSTEMS**

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

## **H.8 GOALS FOR SUBCONTRACTING**

The contractor should leverage this TO to meet Alliant base contract subcontracting goals and assist DHS in meeting its subcontracting goals to the maximum extent possible. Base Alliant and DHS subcontracting goals are restated below.

<b>Small Business</b>	<b>Alliant Goals</b>	<b>DHS Goals</b>
Overall Subcontracting Goal	50%	41%
HUBZone Small Business	3%	3%
Small Disadvantaged Business	6%	5%
Women-Owned Small Business	5%	5%
Veteran-Owned Small Business	3%	--
Service-Disabled Veteran-Owned Small Business	3%	3%

The individual goals of HUBZone Small Business, Small Disadvantaged Business, Women-Owned Small Business, Veteran-Owned Small Business, and Service-Disabled Veteran-Owned Small Business are a subset of the overall small business goals.

Additionally, the contractor shall meet the small business subcontracting goals stated in Section J, Attachment D (AFDP). The goals will be reflect the contractor's unique approach to forming an effective team to deliver HSDN and C-LAN services.

## **H.9 TRAVEL**

### **H.9.1 TRAVEL REGULATIONS**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
- b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

### **H.9.2 TRAVEL AUTHORIZATION REQUESTS (TAR)**

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, activity, and estimated cost. Prior to any long-distance travel in support of any ROM and/or RFC effort, the contractor shall submit its travel estimate via the RFC template (Section J, Attachment P) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR and to the DSSR for work overseas.

Requests for travel approval shall:

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- a. Be prepared in a legible manner.
- b. Include a description of the travel proposed including a statement as to activity.
- c. Be summarized by traveler.
- d. Identify the TO number.
- e. Identify the CLIN associated with the travel.
- f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

### **H.10 TOOLS (HARDWARE/SOFTWARE) AND/OR ODCs**

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall follow the SENS3 Request for Change (RFC)/Technical Direction (TD) Approval Process (Section J, Attachment P). If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the FEDSIM CO a Consent to Purchase (CTP) (Section J, Attachment Q). The RFC and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved TD from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Sections H.11, H.15, and H.16.

### **H.11 COMMERCIAL SUPPLIER AGREEMENTS**

**H.11.1** The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C.4 and as contemplated in the Tools and ODC CLINs in Section B.4 (included with final TOR) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Software Agreements”). For purposes of this TO, the Software Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14(c)(2).

**H.11.2** The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state, and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor’s cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above. The above rights constitute “other rights and

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

limitations” as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

### **H.12 NEWS RELEASE**

The offeror shall not make any news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

### **H.13 INTELLECTUAL PROPERTY RIGHTS**

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

### **H.14 AWARD FEE**

See the AFDP in Section J, Attachment D.

### **H.15 NATIONAL SECURITY AGENCY REQUIREMENTS**

Technologies for SENS3 shall be procured in accordance with Committee on National Security Systems Policy (CNSSP) No. 11, “National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products.” In addition, technologies shall be procured which have been validated by Common Criteria Testing Labs, in accordance with the National Information Assurance Partnership (NIAP) Protection Profiles (PPs). Where a PP exists but the desired product has not been validated against it, the Government shall direct the desired vendor to have its product validated against the appropriate, corresponding PP. For National Security Systems (NSS) where classified data is being protected at rest or in transit by commercial products, technologies from the Commercial Solutions for Classified (CSfC) Components List shall be used, in accordance with NSA’s published CSfC Capability Packages. It is preferred that contractor be NSA-registered as a CSfC trusted integrator. Capability Packages and the CSfC Components List can be found by visiting the following webpage:

<https://www.nsa.gov/resources/everyone/csfc/>

NIAP-validated products can be found at the NIAP website on the page:

<https://www.niap-ccevs.org/Product/>

### **H.16 SUPPLY CHAIN RISK MANAGEMENT**

#### **H.16.1 CONTRACTOR SAFEGUARDS**

The contractor shall support supply chain protections as defined in the NIST SP 800-53 SA-12 control, which states, “The organization protects against supply chain threats to the information system, system component, or information system service by employing (Assignment: organization-defined security safeguards) as part of a comprehensive, defense-in-breadth information security strategy.” NIST SP 800-53 SA-12 can be located at the NIST website:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

The contractor shall provide the Government with a description of what safeguards it intends for supply chain protections.

**H.16.2 COMPANY INFORMATION REVIEW**

For the purposes of supply chain risk assessment under this TO, the “organization-defined security safeguards” referenced above shall include a CO’s review of any negative findings reported by DHS as a result of the Company Information Review (CIR) conducted by DHS. The contractor is under a continuing obligation to ensure that all responses to the Acquisition Risk Questions (see Section F, Deliverable 12 and Section J, Attachment R, Acquisition Risk Questions) answered in the CIR remain complete, accurate, and up-to-date. The contractor shall promptly notify and submit updated responses to the CO when any change in circumstances of the Contractor or subcontractors warrants a change in the contractor’s or subcontractor’s responses to the acquisition risk questions. In addition, the contractor is under a continuing obligation to promptly disclose to the CO any proposed additional or replacement subcontractors.

## SECTION I – CONTRACT CLAUSES

### **I.1 TASK ORDER CLAUSES**

All applicable and required provisions/clauses set forth in FAR 52.301 automatically flow down to all Alliant TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

### **I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a provision may be accessed electronically at the FAR website:

<http://www.acquisition.gov/far/>

<b>FAR</b>	<b>TITLE</b>	<b>DATE</b>
52.203-14	Display of Hotline Poster(s) (fill in or provide link to client's posters)	OCT 2015
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.215-22	Limitations on Pass-Through Charges - Identification of Subcontract Effort	OCT 2009
52.222-2	Payment for Overtime Premiums	JUL 1990
52.222-41	Service Contract Labor Standards	AUG 2018
52.227-14	Rights in Data – Alt. II and III	MAY 2014
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006

### **I.3 FAR CLAUSES INCORPORATED BY FULL TEXT**

#### **FAR 52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)**

(a) Definitions. As used in this clause--

Covered article means any hardware, software, or service that--

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

## SECTION I – CONTRACT CLAUSES

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

Covered entity means--

- (1) Kaspersky Lab;
- (2) Any successor entity to Kaspersky Lab;
- (3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
- (4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from--

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement. (1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at <https://dibnet.dod.mil/>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil/>.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

**FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN  
TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR  
EQUIPMENT (AUG 2020)**

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People’s Republic of China.

Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

## SECTION I – CONTRACT CLAUSES

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

## SECTION I – CONTRACT CLAUSES

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be

## SECTION I – CONTRACT CLAUSES

incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

### **FAR 52.211-14 NOTICE OF PRIORITY RATING FOR NATIONAL DEFENSE, EMERGENCY PREPAREDNESS, AND ENERGY PROGRAM USE (APR 2008)**

Any contract awarded as a result of this solicitation will be ☐DX rated order; ☒DO rated order certified for national defense, emergency preparedness, and energy program use under the Defense Priorities and Allocations System (DPAS) (15 CFR700), and the Contractor will be required to follow all of the requirements of this regulation.

(End of provision)

### **FAR 52.211-15 DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS (APR 2008)**

This is a rated order certified for national defense, emergency preparedness, and energy program use, and the Contractor shall follow all the requirements of the Defense Priorities and Allocations System regulation (15 CFR 700).

(End of clause)

### **FAR 52.216-7 ALLOWABLE COST AND PAYMENT (JUN 2013)**

(a) Invoicing.

(1) The Government will make payments to the Contractor when requested as work progresses, but (except for small business concerns) not more often than once every 2 weeks, in amounts determined to be allowable by the Contracting Officer in accordance with Federal Acquisition Regulation (FAR) [Subpart 31.2](#) in effect on the date of this contract and the terms of this contract. The Contractor may submit to an authorized representative of the Contracting Officer, in such form and reasonable detail as the representative may require, an invoice or voucher supported by a statement of the claimed allowable cost for performing this contract.

(2) Contract financing payments are not subject to the interest penalty provisions of the Prompt Payment Act. Interim payments made prior to the final payment under the contract are contract financing payments, except interim payments if this contract contains Alternate I to the clause at [52.232-25](#).

(3) The designated payment office will make interim payments for contract financing on the 30th day after the designated billing office receives a proper payment request. In the event that

## SECTION I – CONTRACT CLAUSES

the Government requires an audit or other review of a specific payment request to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the specified due date.

(b) Reimbursing costs.

(1) For the purpose of reimbursing allowable costs (except as provided in paragraph (b)(2) of this clause, with respect to pension, deferred profit sharing, and employee stock ownership plan contributions), the term “costs” includes only—

(i) Those recorded costs that, at the time of the request for reimbursement, the Contractor has paid by cash, check, or other form of actual payment for items or services purchased directly for the contract;

(ii) When the Contractor is not delinquent in paying costs of contract performance in the ordinary course of business, costs incurred, but not necessarily paid, for—

(A) Supplies and services purchased directly for the contract and associated financing payments to subcontractors, provided payments determined due will be made—

(1) In accordance with the terms and conditions of a subcontract or invoice; and

(2) Ordinarily within 30 days of the submission of the Contractor’s payment request to the Government;

(B) Materials issued from the Contractor’s inventory and placed in the production process for use on the contract;

(C) Direct labor;

(D) Direct travel;

(E) Other direct in-house costs; and

(F) Properly allocable and allowable indirect costs, as shown in the records maintained by the Contractor for purposes of obtaining reimbursement under Government contracts; and

(iii) The amount of financing payments that have been paid by cash, check, or other forms of payment to subcontractors.

(2) Accrued costs of Contractor contributions under employee pension plans shall be excluded until actually paid unless—

(i) The Contractor’s practice is to make contributions to the retirement fund quarterly or more frequently; and

(ii) The contribution does not remain unpaid 30 days after the end of the applicable quarter or shorter payment period (any contribution remaining unpaid shall be excluded from the Contractor’s indirect costs for payment purposes).

(3) Notwithstanding the audit and adjustment of invoices or vouchers under paragraph (g) of this clause, allowable indirect costs under this contract shall be obtained by applying indirect cost rates established in accordance with paragraph (d) of this clause.

(4) Any statements in specifications or other documents incorporated in this contract by reference designating performance of services or furnishing of materials at the Contractor’s expense or at no cost to the Government shall be disregarded for purposes of cost-reimbursement under this clause.

(c) Small business concerns. A small business concern may receive more frequent payments than every 2 weeks.

(d) Final indirect cost rates.

## SECTION I – CONTRACT CLAUSES

(1) Final annual indirect cost rates and the appropriate bases shall be established in accordance with [Subpart 42.7](#) of the Federal Acquisition Regulation (FAR) in effect for the period covered by the indirect cost rate proposal.

(2)(i) The Contractor shall submit an adequate final indirect cost rate proposal to the Contracting Officer (or cognizant Federal agency official) and auditor within the 6-month period following the expiration of each of its fiscal years. Reasonable extensions, for exceptional circumstances only, may be requested in writing by the Contractor and granted in writing by the Contracting Officer. The Contractor shall support its proposal with adequate supporting data.

(ii) The proposed rates shall be based on the Contractor's actual cost experience for that period. The appropriate Government representative and the Contractor shall establish the final indirect cost rates as promptly as practical after receipt of the Contractor's proposal.

(iii) An adequate indirect cost rate proposal shall include the following data unless otherwise specified by the cognizant Federal agency official:

(A) Summary of all claimed indirect expense rates, including pool, base, and calculated indirect rate.

(B) General and Administrative expenses (final indirect cost pool). Schedule of claimed expenses by element of cost as identified in accounting records (Chart of Accounts).

(C) Overhead expenses (final indirect cost pool). Schedule of claimed expenses by element of cost as identified in accounting records (Chart of Accounts) for each final indirect cost pool.

(D) Occupancy expenses (intermediate indirect cost pool). Schedule of claimed expenses by element of cost as identified in accounting records (Chart of Accounts) and expense reallocation to final indirect cost pools.

(E) Claimed allocation bases, by element of cost, used to distribute indirect costs.

(F) Facilities capital cost of money factors computation.

(G) Reconciliation of books of account (i.e., General Ledger) and claimed direct costs by major cost element.

(H) Schedule of direct costs by contract and subcontract and indirect expense applied at claimed rates, as well as a subsidiary schedule of Government participation percentages in each of the allocation base amounts.

(I) Schedule of cumulative direct and indirect costs claimed and billed by contract and subcontract.

(J) Subcontract information. Listing of subcontracts awarded to companies for which the contractor is the prime or upper-tier contractor (include prime and subcontract numbers; subcontract value and award type; amount claimed during the fiscal year; and the subcontractor name, address, and point of contact information).

(K) Summary of each time-and-materials and labor-hour contract information, including labor categories, labor rates, hours, and amounts; direct materials; other direct costs; and, indirect expense applied at claimed rates.

(L) Reconciliation of total payroll per IRS form 941 to total labor costs distribution.

(M) Listing of decisions/agreements/approvals and description of accounting/organizational changes.

(N) Certificate of final indirect costs (see [52.242-4](#), Certification of Final Indirect Costs).

## SECTION I – CONTRACT CLAUSES

(O) Contract closing information for contracts physically completed in this fiscal year (include contract number, period of performance, contract ceiling amounts, contract fee computations, level of effort, and indicate if the contract is ready to close).

(iv) The following supplemental information is not required to determine if a proposal is adequate, but may be required during the audit process:

(A) Comparative analysis of indirect expense pools detailed by account to prior fiscal year and budgetary data.

(B) General organizational information and limitation on allowability of compensation for certain contractor personnel. See [31.205-6\(p\)](#). Additional salary reference information is available at [http://www.whitehouse.gov/omb/procurement\\_index\\_exec\\_comp/](http://www.whitehouse.gov/omb/procurement_index_exec_comp/).

(C) Identification of prime contracts under which the contractor performs as a subcontractor.

(D) Description of accounting system (excludes contractors required to submit a CAS Disclosure Statement or contractors where the description of the accounting system has not changed from the previous year's submission).

(E) Procedures for identifying and excluding unallowable costs from the costs claimed and billed (excludes contractors where the procedures have not changed from the previous year's submission).

(F) Certified financial statements and other financial data (e.g., trial balance, compilation, review, etc.).

(G) Management letter from outside CPAs concerning any internal control weaknesses.

(H) Actions that have been and/or will be implemented to correct the weaknesses described in the management letter from subparagraph (G) of this section.

(I) List of all internal audit reports issued since the last disclosure of internal audit reports to the Government.

(J) Annual internal audit plan of scheduled audits to be performed in the fiscal year when the final indirect cost rate submission is made.

(K) Federal and State income tax returns.

(L) Securities and Exchange Commission 10-K annual report.

(M) Minutes from board of directors meetings.

(N) Listing of delay claims and termination claims submitted which contain costs relating to the subject fiscal year.

(O) Contract briefings, which generally include a synopsis of all pertinent contract provisions, such as: contract type, contract amount, product or service(s) to be provided, contract performance period, rate ceilings, advance approval requirements, pre-contract cost allowability limitations, and billing limitations.

(v) The Contractor shall update the billings on all contracts to reflect the final settled rates and update the schedule of cumulative direct and indirect costs claimed and billed, as required in paragraph (d)(2)(iii)(I) of this section, within 60 days after settlement of final indirect cost rates.

(3) The Contractor and the appropriate Government representative shall execute a written understanding setting forth the final indirect cost rates. The understanding shall specify (i) the agreed-upon final annual indirect cost rates, (ii) the bases to which the rates apply, (iii) the periods for which the rates apply, (iv) any specific indirect cost items treated as direct costs in

## SECTION I – CONTRACT CLAUSES

the settlement, and (v) the affected contract and/or subcontract, identifying any with advance agreements or special terms and the applicable rates. The understanding shall not change any monetary ceiling, contract obligation, or specific cost allowance or disallowance provided for in this contract. The understanding is incorporated into this contract upon execution.

(4) Failure by the parties to agree on a final annual indirect cost rate shall be a dispute within the meaning of the Disputes clause.

(5) Within 120 days (or longer period if approved in writing by the Contracting Officer) after settlement of the final annual indirect cost rates for all years of a physically complete contract, the Contractor shall submit a completion invoice or voucher to reflect the settled amounts and rates. The completion invoice or voucher shall include settled subcontract amounts and rates. The prime contractor is responsible for settling subcontractor amounts and rates included in the completion invoice or voucher and providing status of subcontractor audits to the contracting officer upon request.

(6)(i) If the Contractor fails to submit a completion invoice or voucher within the time specified in paragraph (d)(5) of this clause, the Contracting Officer may—

(A) Determine the amounts due to the Contractor under the contract; and

(B) Record this determination in a unilateral modification to the contract.

(ii) This determination constitutes the final decision of the Contracting Officer in accordance with the Disputes clause.

(e) Billing rates. Until final annual indirect cost rates are established for any period, the Government shall reimburse the Contractor at billing rates established by the Contracting Officer or by an authorized representative (the cognizant auditor), subject to adjustment when the final rates are established. These billing rates—

(1) Shall be the anticipated final rates; and

(2) May be prospectively or retroactively revised by mutual agreement, at either party's request, to prevent substantial overpayment or underpayment.

(f) Quick-closeout procedures. Quick-closeout procedures are applicable when the conditions in FAR [42.708\(a\)](#) are satisfied.

(g) Audit. At any time or times before final payment, the Contracting Officer may have the Contractor's invoices or vouchers and statements of cost audited. Any payment may be—

(1) Reduced by amounts found by the Contracting Officer not to constitute allowable costs; or

(2) Adjusted for prior overpayments or underpayments.

(h) Final payment.

(1) Upon approval of a completion invoice or voucher submitted by the Contractor in accordance with paragraph (d)(5) of this clause, and upon the Contractor's compliance with all terms of this contract, the Government shall promptly pay any balance of allowable costs and that part of the fee (if any) not previously paid.

(2) The Contractor shall pay to the Government any refunds, rebates, credits, or other amounts (including interest, if any) accruing to or received by the Contractor or any assignee under this contract, to the extent that those amounts are properly allocable to costs for which the Contractor has been reimbursed by the Government. Reasonable expenses incurred by the Contractor for securing refunds, rebates, credits, or other amounts shall be allowable costs if approved by the Contracting Officer. Before final payment under this contract, the Contractor

## SECTION I – CONTRACT CLAUSES

and each assignee whose assignment is in effect at the time of final payment shall execute and deliver—

(i) An assignment to the Government, in form and substance satisfactory to the Contracting Officer, of refunds, rebates, credits, or other amounts (including interest, if any) properly allocable to costs for which the Contractor has been reimbursed by the Government under this contract; and

(ii) A release discharging the Government, its officers, agents, and employees from all liabilities, obligations, and claims arising out of or under this contract, except—

(A) Specified claims stated in exact amounts, or in estimated amounts when the exact amounts are not known;

(B) Claims (including reasonable incidental expenses) based upon liabilities of the Contractor to third parties arising out of the performance of this contract; provided, that the claims are not known to the Contractor on the date of the execution of the release, and that the Contractor gives notice of the claims in writing to the Contracting Officer within 6 years following the release date or notice of final payment date, whichever is earlier; and

(C) Claims for reimbursement of costs, including reasonable incidental expenses, incurred by the Contractor under the patent clauses of this contract, excluding, however, any expenses arising from the Contractor's indemnification of the Government against patent liability.

(End of clause)

### **FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within +30 days of the end of the period of performance.

(End of clause)

### **FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

- a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
- c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed six years.

(End of clause)

### **FAR 52.225-6 TRADE AGREEMENTS CERTIFICATE (MAY 2014)**

## SECTION I – CONTRACT CLAUSES

(a)The offeror certifies that each end product, except those listed in paragraph (b) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."

(b)The offeror shall list as other end products those supplies that are not U.S.-made or designated country end products.

Other End Products:

Part Number	Country of Origin
Z0XZ000LU	China
LC49HG90DMNXZA	China
403-BBMU	China
461-AAEN	China
Z0Y0005Y	China

(c)The Government will evaluate offers in accordance with the policies and procedures of [part 25](#) of the Federal Acquisition Regulation. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for those products are insufficient to fulfill the requirements of this solicitation.

(End of provision)

### **I.4 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE**

The full text of a provision may be accessed electronically at the GSAM website:

<https://www.acquisition.gov/gsam/gsam.html/>

GSAM	TITLE	DATE
552.212-4	Contract Terms and Conditions-Commercial Items (Alternate II) (FAR Deviation)	JUL 2015
552.215-70	Examination of Records by GSA	JUL 2016
552.228-5	Government as Additional Insured	JAN 2016
552.232.25	Prompt Payment	NOV 2009

## SECTION I – CONTRACT CLAUSES

## SECTION J – LIST OF ATTACHMENTS

### **J.1 LIST OF ATTACHMENTS**

The following attachments are attached (either in full text or electronically at the end of the Task Order) or accessible in the controlled website specified in the Cover Letter.

<b>Attachment</b>	<b>Title</b>	<b>Controlled Website</b>
A	COR Appointment Letter	
B	Acronym List	
C	Incremental Funding Chart (electronically attached .xls)	
D	Award Fee Determination Plan	
E	Functional Requirements	
F	Problem Notification Report	
G	Reserved	
H	Reserved	
I	Deliverable Acceptance-Rejection Report	
J	Reserved	
K	Reserved	
L	Organizational Conflict of Interest Statement	
M	Corporate Non-Disclosure Agreement	
N	Addendum to Corporate Non-Disclosure Agreement	
O	Reserved	
P	Request for Change Template (electronically attached .xls)	
Q	Consent to Purchase (CTP) Template (electronically attached .xls)	
R	Acquisition Risk Questions	
S	Reserved	
T	Reserved	
U	Reserved	
V	Reserved	
W	Performance Work Statement	
X	Service Level Agreements (SLAs)	
Y	Reserved	
Z	Reserved	
AA	Reserved	
BB	Reserved	
CC	Reserved	
DD	Reserved	
EE	Reserved	
FF	Reserved	
GG	Reserved	
HH	Reserved	
II	Reserved	
JJ	Reserved	
KK	Reserved	

SECTION J – LIST OF ATTACHMENTS

Attachment	Title	Controlled Website
LL	Reserved	
MM	Reserved	
NN	Reserved	
OO	Reserved	
PP	Reserved	
QQ	Reserved	
RR	Department of Defense (DOD) DD Form 254	
SS	Reserved	
TT	Alternate COR Appointment Letter	
UU	FAR 52.204-24	
VV	C-LAN DPAS Letter	
WW	HSDN DPAS Letter	

